

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF GEORGIA
ATHENS DIVISION

FILED
U.S. DISTRICT COURT
MIDDLE GEORGIA

2009 APR 13 PM 2:11

In the Matter of the Search of the Property

APPLICATION AND AFFIDAVIT
FOR SEARCH WARRANT

DESCRIBED IN ATTACHMENT A
(CURRENTLY IN THE CUSTODY OF THE
FEDERAL BUREAU OF INVESTIGATION)

NO. 3:09-MJ-0406 (CWH)

I, James W. Cearly, Jr., being duly sworn, depose and say:

I am a(n) Special Agent with the Federal Bureau of Investigation and have reason to believe that ☐ on the person of and/or ☒ on the property or premises known as

See Attachment A,

in the MIDDLE DISTRICT OF GEORGIA, there is now concealed a certain person or property, namely (describe the person and/or property to be seized)

See Attachment B,

which is (state one or more bases for search and seizure set forth under Rule 41(c) of the Federal Rules of Criminal Procedure)

evidence of a crime and contraband illegally possessed,

concerning a violation of Title 18, United States Code, Sections 2252 and 2252A.

The facts to support a finding of PROBABLE CAUSE are as follows:

See Affidavit.

Continued on the attached sheet and made a part hereof. ☒ Yes ☐ No

Signature of Affiant [Signature]

Sworn to and Subscribed Before Me, at Macon, Georgia

This 13th day of April, 2009.

Claude W. Hicks, Jr.
Claude W. Hicks, Jr.
United States Magistrate Judge



A true and certified copy.

This 6-16, 2011
GREGORY J. LEONARD, CLERK
U. S. Dist. Court, MD Ga.

By: [Signature]
DEPUTY CLERK

ATTACHMENT A

1. Toshiba Satellite laptop, model # PSAA8U-OLJO2K, serial # 66085265Q.
2. Seagate Free Agent Desk external hard drive, serial # 2GEVHBMN.
3. Seagate Free Agent Pro external hard drive, serial # 9QJ06PP2.
4. Western Digital, My Book external hard drive, serial # WCASP0050710.
5. Western Digital external hard drive, serial # WCAPD2700641.
6. Seagate external hard drive, serial # 3PM0723B.

ATTACHMENT B
ITEMS TO BE SEARCHED FOR AND SEIZED

- a. images of child pornography and files containing images of child pornography in any form;
- b. information or correspondence pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, that were transmitted or received using computer, some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:
 - i. letters and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and
 - ii. records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
- c. credit card information including but not limited to bills and payment records; and
- d. records or other items which evidence ownership or use of computer equipment found in the above residence, including, but not limited to, sales receipts and bills for Internet access.

AFFIDAVIT

I, James W. Cearley, Jr., a Special Agent (SA) with the Federal Bureau of Investigation (FBI), U.S. Department of Justice, being duly sworn, depose and state as follows:

1. I have been employed as a Special Agent of the FBI for twenty years, and am currently assigned to the Atlanta Division's Athens Resident Agency. The FBI has the responsibility, in part, for investigating Federal violations involving child pornography and child exploitation. As an FBI agent, I have conducted a wide variety of investigations including violent crimes, financial crimes, crimes against children and child pornography. Prior to my employment with the FBI, I was employed by the State of Florida as a Police Officer for four years. I have been the affiant and/or participated in numerous search warrants, many of which involved the seizure of computer equipment.

2. As a federal agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

3. The information provided in this affidavit was obtained from my own investigation and the investigation of other law enforcement officers.

4. I am investigating the activities of the Internet account registered to Shari Laist and Fred Laist, 4 Peregrine Crossing, Savannah, Georgia 31411. As will be shown below, there is probable cause to believe that someone using an Internet account registered to the Laists has received, possessed, and/or distributed child pornography, in violation of Title 18, United States Code, Sections 2252 and 2252A. Investigation revealed that a David Laist is also associated with 4 Peregrine Crossing, Savannah, Georgia 31411.

David Laist is also associated with an address at 425 Riverbend Parkway, Apartment 90, Athens, Georgia 30605.

I am submitting this affidavit in support of a search warrant authorizing a search of computers and computer media obtained during an interview ("knock and talk") of David Laist at 425 Riverbend Parkway, Apartment 90, Athens, Georgia 30605 on March 4, 2009, for the items specified in Attachment B hereto, which items constitute instrumentalities, fruits, and evidence of the foregoing violations. I am requesting authority to search computers and computer media obtained during the "knock and talk" and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of crime.

STATUTORY AUTHORITY

5. This investigation concerns alleged violations of Title 18, United States Code, Sections 2252 and 2252A, relating to material involving the sexual exploitation of minors. Title 18, United States Code, Section 2252(a), prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any visual depiction of minors engaging in sexually explicit conduct when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce. Title 18, United States Code, Section 2252A(a), prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any child pornography, as defined in Title 18, United States Code, Section 2256(8), when such child pornography was either mailed or shipped or transported in interstate or foreign commerce by any means, including

by computer, or when such child pornography was produced using materials that had traveled in interstate or foreign commerce.

a. Title 18, United States Code, Section 2252(a)(1), prohibits a person from knowingly transporting or shipping in interstate or foreign commerce, by computer or mail, any visual depiction of minors engaging in sexually explicit conduct. Under Title 18, United States Code, Section 2252(a)(2), it is a federal crime for any person to knowingly receive or distribute, by computer or mail, any visual depiction of minors engaging in sexually explicit conduct that has been mailed or shipped or transported in interstate or foreign commerce. That section also makes it a federal crime for any person to knowingly reproduce any visual depiction of minors engaging in sexually explicit conduct for distribution in interstate or foreign commerce by any means, including by computer or the mail. Under Title 18, United States Code, Section 2252(a)(4), it is also a crime for a person to possess one or more books, magazines, periodicals, films, or other materials which contain visual depictions of minors engaged in sexually explicit conduct that have been transported in interstate or foreign commerce or that were produced using materials that had traveled in interstate or foreign commerce.

b. Title 18, United States Code, Section 2252A(a)(1), prohibits a person from knowingly mailing, transporting, or shipping child pornography in interstate or foreign commerce by any means, including by computer. Title 18, United States Code, Section 2252A(a)(2), prohibits a person from

knowingly receiving or distributing any child pornography that has been mailed or shipped or transported in interstate or foreign commerce by any means, including by computer. Title 18, United States Code, Section 2252A(a)(3), prohibits a person from knowingly possessing or reproducing child pornography for distribution through the mail or in interstate or foreign commerce by any means, including by computer. Title 18, United States Code, Section 2252A(a)(5)(B), prohibits a person from knowingly possessing any book, magazine, periodical, film, videotape, computer disk, or other material that contains an image of child pornography that has been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer.

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachments A and B to this Affidavit:

- a. "Child Pornography," as used herein, includes the definition in Title 18, United States Code, Section 2256(8), (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of

a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct (see Title 18, United States Code, Sections 2252 and 2256(2)).

b. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See Title 18, United States Code, Section 2256(5).

c. "Computer," as used herein, is defined pursuant to Title 18, United States Code, Section 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

d. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other

memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

e. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

f. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

g. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may

include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

h. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

i. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards

(MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

7. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

8. Persons engaged in the production, communication, distribution and storage of child pornography can transfer photographs from a camera onto a computer-readable format with a scanner. With digital cameras, the images can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world.

9. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

10. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

11. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

12. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

13. A growing phenomenon on the Internet is peer to peer file sharing (P2P). P2P file sharing is a method of communication available to Internet users through the use

of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up file(s) on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user's computer, and conducting searches for files that are currently being shared on another user's computer.

14. Gigatribe, one type of P2P software, allows users to setup their own private P2P network of contacts. File sharing through Gigatribe is limited to only other users who have been added to your private list of "friends". A new user is added to your list of friends through a friend request. Acceptance of a friend request will allow that new user to download file(s) from the user who sent the friend request. The new user can then browse the list of files the other user has available to download, select the file(s) from this list, and download the selected file(s). The download of a file is achieved through a direct connection between the computer requesting the file and the computer containing the file.

15. One of the advantages of P2P file sharing is that multiple files may be downloaded in parallel. This means that the user can download more than one file at a time.

16. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address, expressed as four sets of numbers separated by decimal points, is unique to a particular computer during an online session. The IP address provides a unique location making it possible for data to be transferred between computers.

17. Third party software is available to identify the IP address of the P2P computer sending the file. Such software monitors and logs Internet and local network traffic.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

18. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally difficult to accomplish this kind of data search on site; and

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is

difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

19. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

20. In addition, there is probable cause to believe that the computer and its storage devices are all instrumentalities of the crime(s), within the meaning of Title 18, United States Code, Sections 2251 through 2256, and should all be seized as such.

SEARCH METHODOLOGY TO BE EMPLOYED

21. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following

techniques (the following is a non-exclusive list, as other search procedures may be used):

- a. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;
- b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- c. surveying various file directories and the individual files they contain;
- d. opening files in order to determine their contents;
- e. scanning storage areas;
- f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and/or
- g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

BACKGROUND OF THE INVESTIGATION

22. By way of background, an FBI agent acting in an undercover capacity as part of an ongoing Innocent Images National Initiative, conducted several online undercover sessions between July 9, 2008, and July 11, 2008. These sessions identified several U. S. and foreign persons utilizing Usenet newsgroups (alt.binaries.jerry, alt.binaries.chakotay and alt.binaries.jtp) to distribute child pornography (CP) images and videos. This information was forwarded to the Innocent Images Unit (IIU) for the purpose of organizing a coordinated takedown to include the execution of search/and or arrest warrants for the subjects. On July, 11, 2008, while conducting online undercover session UMP-200, the undercover agent entered the publically accessible newsgroup alt.binaries.chakotay and observed that multiple users had made posts with titles associated with CP. The agent observed a user name "Tarheel" had posted approximately 230 images under the subject line: "2.jpg – trying again, just a thank you, hope some are new, fills appreciated (1/1)". This message was date/time stamped 2 Jul 2008 23:08:01-0500. Header information in the post indicated it was posted through the news provider Newscene.com. Thereafter, the agent downloaded the images posted by Tarheel. Upon review, the agent found the images depicted prepubescent and pubescent boys exposing their genitalia, masturbating, and performing oral sex. A subpoena was served to Novia Corporation/Newscene.com who subsequently advised that the message IDs contained in the header of Tarheel's post resolved to an account in the name of Shawn Hodge, e-mail address fruiti_elias@yahoo.com, address 34 Elm Street, Allentown Pennsylvania 18106, posting 70.157.179.204, customer since January 22, 2007. Novia Corporation/Newscene.com

confirmed that Internet Protocol (IP) address 70.157.179.204 was associated with the images posted by Tarheel in the newsgroup. However, Novia Corporation/Newsscene.com advised that the identifying information is provided by the customer and is not verified by the company. An administrative subpoena served on Yahoo! for the e-mail address fruti_elias@yahoo.com returned what appeared to be fictitious information. Yahoo! was able to determine that the email account was registered on December 17, 2006, via IP address 72.155.48.137. Public records checks conducted on Shawn Hodge listed an address of 132 N. Greenwood, in Tamaqua, Pennsylvania, approximately 32 miles from Allentown, Pennsylvania. A review of billing records provided by Novia Corporation/Newsscene.com indicated that the account was opened and paid via American Express card# 3790174138360960808. American Express advised that this was a gift card purchased on January 22, 2007, at Kroger's Store #255, located at 2301 College Station Road, Athens, Georgia. A follow-up subpoena was served to Bell South Telecommunications for the subscriber of the account accessing IP address 70.157.179.204 at the date/time Tarheel posted the images of CP in the newsgroup. Bell South advised that the IP address was associated with Shari Laist and Fred Laist, email address laists@bellsouth.net, address 4 Peregrine Crossing, Savannah, Georgia 31411, telephone number 912-598-1346. A query of LexisNexis revealed that Fred Laist, Shari Laist and David Laist are currently associated with this address. Furthermore, public records indicated that David Laist was associated with 425 Riverbend Parkway, Apartment 90, Athens, Georgia, from August 2006 through December 2007. This address was determined to be approximately 2.9 miles from the Kroger's store where the American Express gift card,

which was used to set up the Newscene.com account, was purchased in January, 2007. Subsequent investigation revealed that David Laist is currently enrolled at the University of Georgia and residing at 425 Riverbend Parkway, Apartment 90, Athens, Georgia 30605. It should be noted that the IP address was used in July 2008, when school is usually adjourned, to post the CP.

23. At approximately 6:00am, March 4, 2009, FBI SA's James W. Cearley, Jr., John A. Sherrill, Jr., along with FBI CART Examiner Orlando Figueroa, observed David Laist standing outside his residence, 425 Riverbend Parkway, Apartment 90, Athens, Georgia 30655. Agents approached Laist, advised of their identity and nature of business. Laist invited agents inside his residence and into his bedroom. Laist's bedroom was separated from other bedrooms inside the residence by a door containing a bolt lock. Laist advised that the bedroom that he led us to was his and the laptop computer and external hard drives contained within the bedroom were his and only he had access to them. Laist advised that he had downloaded CP images from the Internet in the past to his Toshiba laptop computer and five (5) external hard drives that were observed by affiant to be connected to the laptop, which are described as follows: Toshiba Satellite laptop, model # PSAA8U-OLJO2K, serial # 66085265Q; Seagate Free Agent Desk external hard drive, serial # 2GEVHBMN; Seagate Free Agent Pro external hard drive, serial # 9QJ06PP2; Western Digital, My Book external hard drive, serial # WCASP0050710; Western Digital external hard drive, serial # WCAPD2700641; and Seagate external hard drive, serial # 3PM0723B. He advised that he would connect directly into shared folders/servers located on other's computers/servers using his laptop computer. Laist described his downloading of CP as being from passive

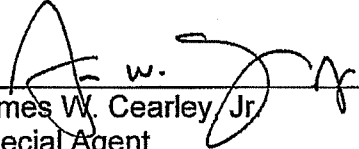
systems, where everything is available as a shared entity. Laist admitted that his computer laptop and five (5) external hard drives currently contained CP. Laist stated that he is on-line, via the internet, 24/7, that CP is available 24/7 and described his access to and downloading of CP to be more than occasionally. Laist stated that he last downloaded CP on March 3, 2009. Laist advised that he was concerned that admitting to possession of CP would endanger his ability to obtain a job after he graduates from the University of Georgia Pharmacy School. Laist read and signed a FD-26/Consent to Search and a FD-941/Consent to Search Computer(s). Laist advised that he wanted to fully cooperate in the future and provided his Account/User Name as dingbat69 and his Password as Sirius and the program he utilizes as Gigatribe 2.46. CART Examiner Figueroa was able to access Laist's laptop computer using the information provided by Laist and identified an image of CP (1575.jpg/young white male with someone's erect penis in his hand), which was observed by agents. Laist also read and signed a Consent to Assume Online Presence. Laist released the previously described Toshiba laptop computer and five (5) external hard drives to agents and was given a copy of FD-597/Receipt for Property. On March 5, 2009, Laist telephonically contacted agent to provide his TrueCrypt (security program operated off of his laptop computer) password, davidisanerddavidisanerd, to access/open encrypted operational files from his external hard drives.

CONCLUSION


24. Based on the aforementioned factual information, your affiant respectfully submits that there is probable cause to believe that David Laist is involved in possession and/or distribution of child pornography. Your affiant respectfully submits

that there is probable cause to believe that Laist has violated Title 18, United States Code, Sections 2252 and 2252A. Additionally, there is probable cause to believe that evidence of the commission of criminal offenses, namely, violations of Title 18, United States Code, Sections 2252 and 2252A, is contained on the laptop computer and five (5) external hard drives which were released to agents on March 4, 2009, by David Laist and listed in Attachment A to this affidavit.

25. Your affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search and seizure for the items listed in Attachment B.


James W. Cearley Jr.
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me
this 13th day of April, 2009.


CLAUDE W. HICKS, JR.
UNITED STATES MAGISTRATE JUDGE